SimpleSAMLphp

SimpleSAMLphp is an open-source implementation for federated AAI based on SAML.

- Ownership: UNINETT
- Documentation: https://simplesamlphp.org/docs/stable/
- Licence: LGPL 2.1
- Source code: https://github.com/simplesamlphp/simplesamlphp

- Features
- Supported Standards
- User Interfaces and APIs
- Support for Virtual Organisations
- Dependencies and other technologies
- Operational Overview
- Expected level of support

Features

SimpleSAMLphp primarily focuses on providing support for SAML2 SPs and IdPs.

At the same time, SimpleSAMLphp supports other identity protocols and frameworks, such as Shibboleth 1.3, A-Select, CAS, OpenID, ADFS, WS-Federation or OAuth. It also supports popular social media identity providers, such as Facebook, LinkedIn, MySpace, Twitter and Windows Live. SimpleSAMLphp is easily extendable due to its modular architecture. Some of the most important extension points of SimpleSAMLphp include:

- Authentication Modules: For implementing custom authentication methods, such as PKI-based, or using proprietary user data sources.
- Authentication Processing Filters: To allow any kind of processing right after authentication has taken place.
- Themes: To customise the look of any page served by SimpleSAMLphp by modifying the CSS, headers, and footers.
- Modules: For extending SimpleSAMLphp with new identity protocols, pages, registry systems etc.

SimpleSAMLphp comes with a number of built-in modules, authentication modules and processing filters that may be used as is, or modified to fit specific needs. It also provides:

- an abstract datastore API, allowing alternative ways of storing data
- an abstraction layer of metadata handling, allowing alternative implementations of metadata consumption
- multiple session handlers, e.g. PHP built-in session handling or Memcache
- step-up authentication based on different Levels of Assurance

Apart from the modules that ship by default with SimpleSAMLphp, a number of extra modules have been made available by third-party developers covering specific features. A non-exhaustive list of such modules follows:

- Attribute Authority: Provides back-end SAML Attribute Authority functionality
- Attribute Aggregator: Supports attribute aggregation as an Authentication Processing Filter.
- Content Simple Admin: Implements a very simple user interface for managing user consent.
- Kerberos: Enables Kerberos 5 authentication.
- Metadata aggregator2: Aggregates a set of SAML entities into SAML2 metadata documents
- Metaedit: Allows basic editing of metadata, as well as manually registering metadata for service providers.
- OAuth 2.0: Adds support for the OAuth 2.0 protocol.
- OpenID Consumer: A module adding support for the OpenID protocol as a Consumer.
- OpenID Provider: A module adding support for the OpenID protocol as an Identity Provider.
- Selfregister: Allows registration of users accounts.
- VOOT Groups: Allows retrieving group memberships from an API service protected with OAuth 2.0 using the VOOT protocol and adds this information to the list of attributes received from the IdP.

- Attribute Aggregator module (developed by NIIF): Issues SAML2 AttributeQuery to an Attribute
- Authority that supports SAML2 SOAP binding
- Attribute-from-rest-api module (developed by NIIF): Requests attributes from REST API in JSON forma

Supported Standards

SAML2/1.1, OpenID, OAuth 2.0, Kerberos, VOOT, SQL, LDAP, RADIUS

User Interfaces and APIs

- Web-based UIs

- SAML SP/IdP metadata in XML exposed through HTTP
- PHP-formatted configuration files

Support for Virtual Organisations

Using the third-party VOOT Groups module, SimpleSAMLphp can retrieve group memberships from an API service protected with OAuth 2.0 using the VOOT protocol and add this information to the list of attributes received from the IdP.

Dependencies and other technologies

- Written in PHP
- Runs on a wide variety of web servers (Apache, nginx and IIS among others)
- Can utilise a user repository based on a SQL database (e.g. MySQL or PostgreSQL), an LDAP directory (OpenLDAP) or a RADIUS interface (OpenRADIUS).
- Can maintain session information in memcached servers for improving performance/high availability

Operational Overview

As simpleSAMLphp is written in PHP, integrating Web-based PHP applications into a federation is very simple. However, simpleSAMLphp also supports non-PHP environments by adding a special cookie in Memcache suitable for the Apache “Auth Memcookie” module. This approach allows passing authentication information in HTTP header variables and enables authorisation via the Apache server configuration. Memcache can also be used to allow an arbitrary number of SimpleSAMLphp web front-ends to work with a back-end matrix of Memcache servers in support of both replication (fail-over) and load-balancing capabilities.

To connect the same SP to multiple IdPs, simpleSAMLphp offers two built-in SAML2 IdP Discovery Services: a basic (enabled by default) and a more advanced one providing scalable search capabilities (please refer to Section 3.10). To act as an IdP, simpleSAMLphp can be configured to utilise a user repository based on a SQL database (e.g. MySQL or PostgreSQL), an LDAP directory or a RADIUS interface.

Expected level of support

SimpleSAMLphp has a large user base, a helpful user community and a number of external contributors .

The AARC requirements supported by the tool are:

- Federation solutions based on open and standards-based technologies